পঞ্জীভুক্ত নম্বৰ - ৭৬৮ /৯৭ Registered No.-768/97

অসম ৰাজপত্ৰ

সত্যমেব জয়তে

THE ASSAM GAZETTE

অসাধাৰণ

EXTRAORDINARY

প্ৰাপ্ত কৰ্ত্তৃত্বৰ দ্বাৰা প্ৰকাশিত

PUBLISHED BY THE AUTHORITY

নং 349 দিশপুৰ, শনিবাৰ, 31 জুলাই, 2021, 9 শাওণ, 1943 (শক)

No. 349 Dispur, Saturday, 31st July, 2021, 9th Sravana, 1943 (S. E.)

GOVERNMENT OF ASSAM
ORDERS BY THE GOVERNOR
INFORMATION TECHNOLOGY DEPARTMENT

NOTIFICATION

The 8th July, 2021

No. IT.51/2009/386.- The Governor of Assam is pleased to notify the Assam Cyber Security Policy, 2020 for the State of Assam framed in consultation with concerned Departments of the Government of Assam.

The Assam Cyber Security Policy is appended herewith.

Assam Cyber Security Policy 2020

1. Purpose

The purpose of this policy is to provide the Government of Assam with the necessary direction, support and security framework requirements to protect the digital information and Information Communication Technology asset of the State. The protection extends to data and ICT asset of all the Departments and its constituent organizations, based on their administrative and electronic services delivery requirements.

This policy shall meet the minimum cyber security requirements in order to protect the confidentiality, integrity and availability of state-owned electronic information by Departments and its constituent organizations. It also shall meet the required assurance and the acceptable level of asset protection from external and internal threats.

2. Vision

To ensure, promote and sustain a safe and resilient cyberspace in the State to promote well-being of the Government, Citizen and Business.

3. Mission

To identify, analyze, protect and build capabilities to prevent and respond to cyber threats posed on State's digital information and ICT asset in Cyber Space through a combination of institutions, people, processes, technology and cooperation.

4. Objective

This Policy shall serve as best practice in information security for all the Departments and constituent organizations of the Government of Assam. This policy shall include all aspects of management including direction and support for information security in accordance with the pertinent sections of various Acts, Rules and Guidelines of the Government of India. The following are the objectives of the policy

4.i **Protection of Digital Information and Information Infrastructure:** Protect the Government digital information of Assam as well as the data within its custody and safeguarding its confidentiality, integrity and availability. Also, to identify, notify and protect Information Infrastructure of the Government of Assam and establish necessary institutional mechanism for safeguarding the information and resources from theft, abuse, misuse and any form of damage.

4.ii Create Awareness and Build Capacity: To develop capacity and create awareness amongst the employees of the Government of Assam for a cyber secured culture in order to minimize the occurrence and severity of information security incidents.

4.iii Setup Institutional Security Governance: To establish responsibility and accountability to oversee management of information security and promote cyber security ecosystem in the State.

5. Strategies to meet the objectives

5.i Protection of Digital Information and Information Infrastructure

To meet the objectives mentioned in the para 4.i the following strategies are formulated

a) Identification and Assessment of Information Infrastructure using risk base assessment. Based on risk parameters, expert judgement and estimation etc. the information infrastructure shall be grouped as critical or non-critical for Government processes.

b) Ensure carrying out Risk (Vulnerability-Threat- Impact) Analysis for the security of data as per data security architecture, standards within one year of notification of the policy. Further, Risk Analysis shall be initiated whenever there is significant change or upgrade in the system.

c) Apply Security Controls as per requirements. Ensure Security Controls is taken as a key design parameter for all ICTs projects throughout the project lifecycle from conceptualization phase.

d) Plan, develop, maintain and review documented process for IT Security Service Level Agreements. The same shall be strictly followed while designing the Service Level Agreements with service providers including Cloud Service Providers (Public or Private).

e) Plan, establish, implement, operate, monitor, review, maintain and continuously improve the Information Security Management System (ISMS) or industry accepted standards, frameworks as per latest guidelines for protection of digital information.

f) Ensure periodic conduct of internal and external Information Security Audits according to the requirements of the organization based on ISMS.

g) All non-critical ICT assets of the Departments and constituent organizations shall be duly protected and monitored through necessary institutional setup and Incident Management Systems.

h) Plan, develop, maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, communication devices, servers, systems and services supporting information infrastructure. The logs shall be handled as per the best practice of Information Security requirements.

i) The Government of Assam shall declare the identified Critical Information Infrastructure of the concerned Departments and Constituent organizations vide necessary Gazette notification within 180 days of time from notification of this policy.

j) Develop Incident Response Plan and Cyber Crisis Management Plan for all Critical and Non-Critical Information Infrastructures of Constituent organizations.

k) Ensure Disaster Recovery and Business Continuity Planning (BCP) security Controls for minimum downtime and the restoration process.

l) Ensure all e-Governance applications including other Government applications such as geospatial applications, websites, portal etc. should be hosted at the Assam State Data Center (ASDC) and shall use Assam State Wide Area Network (ASWAN) as per availability or any other secure network at different level (SHQ – DHQ – BHQ). For secure operation of ASDC and ASWAN, the following detailed guidelines shall be issued by Information Technology Department separately.

   i. Assam State Data Centre (ASDC) Usages Guidelines including hosting of application, cloud provisioning, backup of data & retention rules and security requirements etc. of user Departments.

   ii. Assam State Wide Area Network (ASWAN) Guidelines including security requirements etc. of user Departments.

   iii. Develop a Data Repository Guideline for the Government of Assam to facilitate the sharing and utilization of data for analytical and research purpose as per National Data Sharing and Accessibility Policy NDSAP 2012.

m) Ensure security certification on procurement of IT security product / critical IT infrastructures / services. Any product / service blacklisted by Government of India for cyber security reasons, should be complied under this policy.

n) Establish best practices for secure disposal of ICT assets phased out by the Departments and its constituent organizations.

o) Maintain the documentation of the above operating procedures ensuring version control. All the operating procedures should be periodically reviewed in order to ensure their effectiveness and adherence.

5.ii Awareness and Capacity Development

Capacity development programmes shall be conducted to create awareness, knowledge enhancement and skill development in understanding the ever-increasing intricate technological changes and mitigating the consequent vulnerabilities.

a) Take appropriate measures for continuous enhancement of the awareness levels of State Government employees on security of ICT assets, processes and information.

b) Identify and assess the knowledge and skill gap at various levels at regular intervals.

c) Develop curricula on security trainings and design training programs.

d) Perform periodic evaluation of the training strategies, programs and outcomes.

5.iii Setup Institutional Security Governance

The Government of Assam under this Policy shall create necessary Apex Level, Departmental Level and District Level Security Governance Structures in time bound manner to ensure adequate planning, identification and compliance for ensuring cyber security of the State at different levels.

a) Constitute Apex Committee for State Cyber Security under the chairmanship of Chief Secretary for providing strategic direction, guidance and coordinate matters related to information security in the State within 30 days from the Gazette notification of this Policy.

b) Constitute Department Level Cyber Security Steering Committee, under the chairmanship of Senior-most Secretary of the Department to ensure information security within 45 days from the Gazette notification of this Policy.

c) Constitute District Level Cyber Security Steering Committees, under the chairmanship of the Deputy Commissioners of the districts within 60 days from the Gazette notification of this Policy.

6. Role of Information Technology Department

Information Technology Department, Government of Assam shall be the nodal Department for administering this policy and have the authority to implement and modify this policy under the direction and guidance of the Apex Committee. Information Technology Department shall formulate required guidelines, issue notifications and set up monitoring mechanism for the implementation of this Policy.

The major roles and responsibilities of the Information Technology Department are as follows:

i. Coordinate with Apex Committee, Department Level Security Steering Committee and District Level Security Steering Committee for implementation of the Policy.

ii. Implementation of the Strategies to meet the objectives of the Policy for the key ICT asset under the Information Technology Department.

iii. Constitute a Cyber Security Division in Directorate of Information Technology, Electronics and Communication (DITEC) to oversee the security implementation and audit related activities in the State.

iv. Provide necessary support to all the Departments in implementing their security strategies in respect of Digital Information and Infrastructure to align with the objectives of the Policy.

v. Information Technology Department shall create necessary mechanism with the support of organisations of Government of India like Cert-In and NCIIPC to issue the advisory for protection of ICT assets including Critical and Non Critical ICT assets for the other Departments.

vi. Information Technology Department shall develop and implement Incident Response Plan and Cyber Crisis Management Plan for the State and engage resources to handle cyber incident and cyber crisis for the Information Technology Department and extend support to other Departments in implementing the same.

vii. Develop the capacity for administering the internal security audit and empanel security audit firms for third party security audit for all Departments.

viii. Identify, develop and conduct courses and certification programme for imparting training to the officials of Government of Assam at different level.

ix. Develop and conduct State wide Cyber Security awareness program for electronic service delivery.

x. Adoption of emerging technologies like IoT, Artificial Intelligence, Blockchain for ensuring Cyber Security in the State.

xi. Detail guidelines shall be prepared by the Information Technology Department to define the functioning, roles and responsibilities of the Committees constituted in consultation with the concerned authorities.

7. Role of Government Departments/Organizations

The roles and responsibilities of various Departments/Organizations of Government of Assam are as follows:

i. Nominate CISO for the Department and its constituent agencies.

ii. Implementation of the Strategies to meet the objectives of this Policy.

iii. Implement the advisory of Information Technology Department regarding protection of Critical and Non Critical ICT assets of the Department.

iv. Develop Incident Response Plan and Cyber Crisis Management Plan with requisite team to handle cyber incident and cyber crisis.

v. Administer the internal security audit by the Department or seek support from Information Technology Department.

vi. Conduct 3rd party security audit through empaneled agencies of Information Technology Department or any other competent agencies.

vii. Department may adopt emerging technologies like Artificial Intelligence, Machine Learning, Blockchain for ensuring Cyber Security. For any such initiatives, the Departments shall inform Information Technology Department throughout the project lifecycle from conceptualization phase.

8. Apex Committee for State Cyber Security

The Information Technology Department shall constitute an Apex Committee under the Chairmanship of Chief Secretary, Government of Assam within 30 days from Gazette notification of this policy.

The constitution of the Committee shall have the following members

i.Chairperson:

Chief Secretary, Government of Assam

ii. Member Convenor:

Senior most Secretary, Information Technology Department, Government of Assam.

iii. Members:

a) Senior most Secretary, Finance Department, Government of Assam
b) Senior most Secretary, Home & Political Department, Government of Assam
c) Senior most Secretary, T&D Department, Government of Assam
d) Senior most Secretary, AR&T Department, Government of Assam
e) Senior most Secretary, Personnel Department, Government of Assam

f) DGP, Assam Police, Government of Assam or representative not below the rank of ADGP.
g) The Director, Directorate of Information Technology, Electronics and Communication (DITEC), Government of Assam.
h) State Informatics Officer, National Informatics Center.
i) Managing Director, AMTRON.
j) Chief Information Security Officer (CISO), Information Technology Department, Government of Assam.
k) Representative from NCIIPC / CERT-In, Government of India.
l) Representative from other Departments as needed.

The Chairperson may nominate domain experts from Industry and Academia as members of the committee.

Key Functionality:

i. Provide guidance with regard to the strategic inputs at the policy level.
ii. Notification of Critical Information Infrastructure.
iii. Declaration of Cyber Crisis and In-Crisis Management.
iv. Review and monitor the progress from time to time and provide guidance related to required changes.
v. Approval of fund to carry out implementation and monitoring of Cyber Security in the State.
vi. Meeting of the Apex Committee shall be held in every six months of the calendar year.
vii. Recommendation for Policy review.

9. Department Level Cyber Security Steering Committee

A Department Level Cyber Security Steering Committee under the Chairpersonship of Senior most Secretary of the Department shall be constituted within forty five days (45) of the notification of this policy with following constitution:

i. **Chairperson:**
Senior most Secretary of the Department
ii. **Members:**
a) Chief Information Security Officer (CISO) of the Department.
b) Nodal officer or Head of the IT Project of the Department.
c) Financial Advisor to the Department.
d) Technical in-charges (System, Network and Database Administrator etc.).

Key Functionality:

i. Implementation of the Policy in the Departments.
ii. Do In-Crisis Management.
iii. Review and monitor the implementation of Cyber Security in the Department.

10. District Level Cyber Security Steering Committee

A district Level Cyber Security Steering Committee under the chairpersonship of Deputy Commissioner of the district shall be constituted.

i. Deputy Commissioner
ii. Addl. Deputy Commissioner (e-Governance)
iii. Superintendent of Police
iv. District Informatics Officer, NIC
v. District Manager of Directorate of Information Technology, Electronics and Communication (DITEC)
vi. Representative from AMTRON and any other IT projects as needed.

Key Functionality:

i. Implementation of the Policy in the respective District.
ii. Do in-Crisis Management.
iii. Review and monitor the implementation of Cyber Security in the District.

11. Budget Allocation for the Implementation of the Policy

All Departments implementing and maintaining IT projects may allocate appropriate funds for cyber security. This budget allocation by the Departments shall be utilized as per the policy and guidelines of the State.

In case of major funding is needed for Cyber Security requirements of the State necessary approval shall be obtained from the Apex Committee.

12. Operative Period of Policy

The Assam Cyber Security Policy, 2020 shall be operative from the date of Gazette Notification.

13. Policy Review

The Policy shall be further reviewed by Information Technology Department consequent to the issuance of National Cyber Security Strategy 2020-25 and as per change in security scenario.

Glossary of Terms Used

Term	Full Form/Meaning
Act	Information Technology Act 2000 and subsequent amendments.
Agency	Organization that is involved in business interest with the State Government or is handling any government related data.
Antivirus	Software designed to detect and destroy computer viruses.
Cert-In	Computer Emergency Response Team-India.
CII	Critical Information Infrastructure (CII).
Cyber Security	Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access use, disclosure, disruption, modification or destruction.
Department	The Administrative Department under the Government of Assam as specified in the Assam Rules of Executive Business, 1968.
GoI	Government of India.
Government	Government of Assam.
ICT Asset	Information and Communication Technology infrastructure
Incident	Security event that changes or affects the everyday operations of an informatic technology service, indicating that a may have been violated or a securit safeguard may have failed.
Information Security	Practice of protecting information from unauthorized access, use, disclosur disruption, modification, perusal, inspection, recording or destruction.
ISMS	Information Security Management System.
IT Audit	Process of collecting and evaluating evidence to determine whether a comput system has been designed to maintain data integrity, safeguard asset, allo organizational goals to be achieved effectively, and uses resources efficiently.
IT Department	Information Technology Department, Government of Assam.
NCIIPC	National Critical Information Infrastructure Protection Centre.
Official Gazette	Official gazette of the Government.
Organizations	Departments and its constituent agencies and institutes of Government of Assam.
Policy	Statement of intent, and is implemented as a procedure or protocol.
State	State of Assam.
SHQ-DHQ-BHQ	State Head Quarter, District Head Quarter, Block Head Quarter.

All other words and expressions used but not defined in this policy, but defined in the Inform Technology Act, 2000 (and amendment 2008) or National Cyber Security Policy 2013 ar guidelines and/or rules and regulations made thereunder shall have the same meanin respectively assigned to them in such Acts and/or policy and/or guidelines and/or rules regulations, as the case may be.

NIRAJ VERMA,
Principal Secretary to the Government of Assam,
Information Technology Department.

Guwahati : Printed and Published by the Director, Directorate of Printing & Stationery, Assam, Guwahati-21.
Extraordinary Gazette No. 697 - 100 + 10 - 31 - 07 - 2021. (visit at– dpns.assam.gov.in)